EXHIBIT 254

Cybersecurity Considerations for Voting Systems

Wenke Lee, Ph.D.

wenke.lee@gmail.com

Wenke Lee

- Work at Georgia Tech (2001-)
  - Professor of Computer Science, John P. Imlay Jr. Chair
  - Co-Executive-Director of the Institute for Information Security & Privacy (IISP)
  - Teach cybersecurity to 2,500 students/year
- Researcher in cybersecurity (1994-)
  - Ph.D. in 1999 from Columbia University (Thesis: a machine learning framework for intrusion detection)
  - Systems and network security, malware analysis, botnet detection, cryptography; Damballa (Core Security)

SAFE Commission

- Work and opinion: my own
- Input from researchers in voting system security

Vulnerabilities in Voting Systems

- There will always be … not news!
- Vulnerabilities = errors/weaknesses that can be exploited by attackers

- No system can be shown to contain no error
  - Developed by engineers/programmers
    - Chrome: 7 million lines of code, Android: 15 million, Windows: 50 million, Car: 100 million+
  - *Can you write/edit a book that thick without an error?*

EVERY System Is at Risk

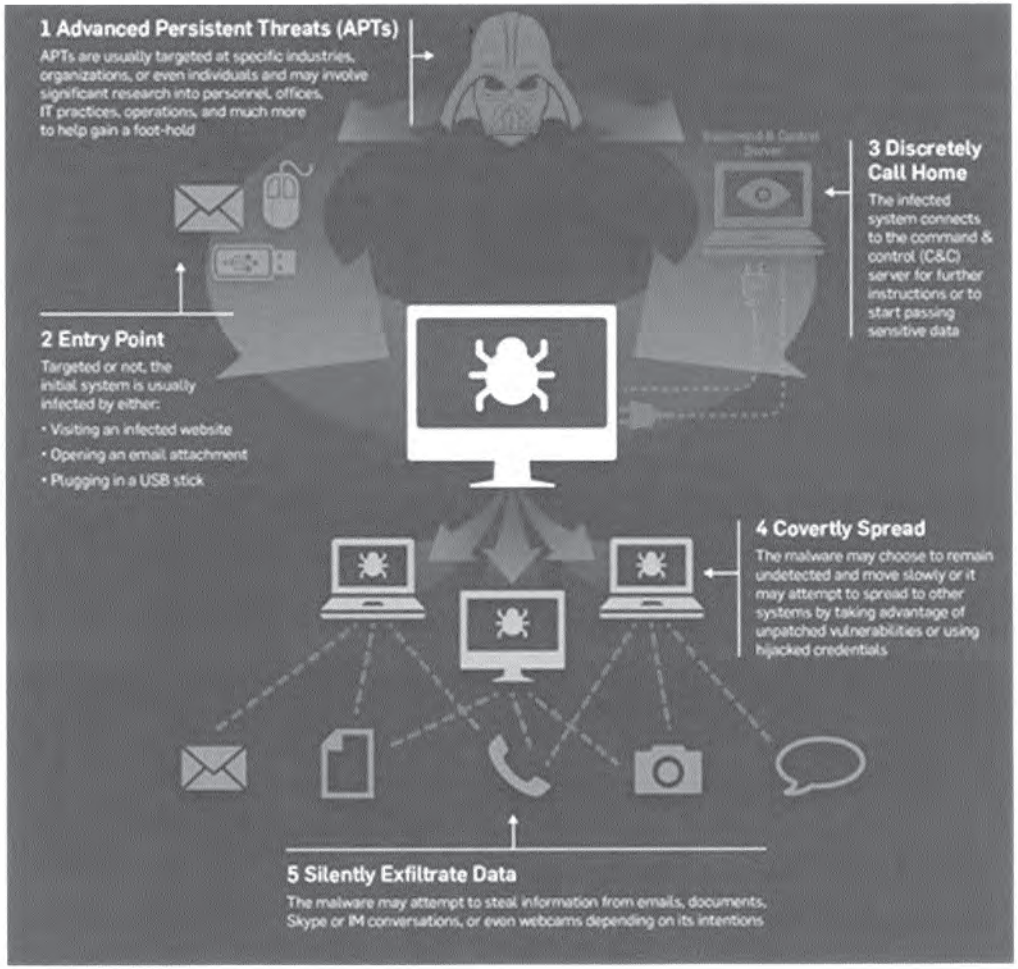
- Not if but when, how much can we find out?

- Even sophisticated, high-profile organizations have been attacked
  - E.g., OPM, HomeDepot, Equifax

- Many organizations seek public help to secure their systems
  - DoD, Google, Apple, Tesla, United Airlines

Cybersecurity Is VERY Hard

Advanced Persistent Threats



Achieving Cybersecurity

- Secure = not vulnerable to cyber attacks
- Option #1: don't use any cyber component
  - Because we can't guarantee no vulnerability
- Option #2: keep away would-be attackers
  - But the cyber world is VERY connected
    - E.g., from Internet-facing system to "disconnected" system via media (e.g., Stuxnet)
  - "Insider" attacks
    - Compromised account = insider

Achieving Cybersecurity

- Option #3: be practical (not absolute 0 or 1)
  - *Security* is a state of well-being for information and infrastructures in which the possibility of successful yet *undetected* theft, tampering, and disruption of information and services is kept low or *tolerable*
    - Confidentiality, authenticity, integrity, availability

Achieving Cybersecurity

- The security life cycle
  - *Iterations* of
    - Threat and risk analysis
    - Policy decisions
    - Specification
    - Design
    - Implementation
    - Operation and maintenance

Cybersecurity in Voting Systems

- Threat and risk analysis
  - "Rank order" threats based on
    - Impact, success probability, attribution potential
    - Can a remote attacker change MANY votes?
      - And what are the components that can be targeted?
    - Can a few attackers with access (e.g., posed as worker or voter) change MANY votes?
    - Can a remote attacker shutdown (i.e., make unavailable) the key components (e.g., reporting)?
    - Etc.

Cybersecurity in Voting Systems

- Policy decisions
  - What is really important? Or, what risks can we tolerate (and to what extent) and what can't we?
  - Integrity: votes are accurately counted
  - Voter confidence:
    - Verifiably cast-as-intended
    - Verifiably collected-as-cast
    - Verifiably counted-as-collected

    - *Any* cyberattack can erode voter confidence

Cybersecurity in Voting Systems

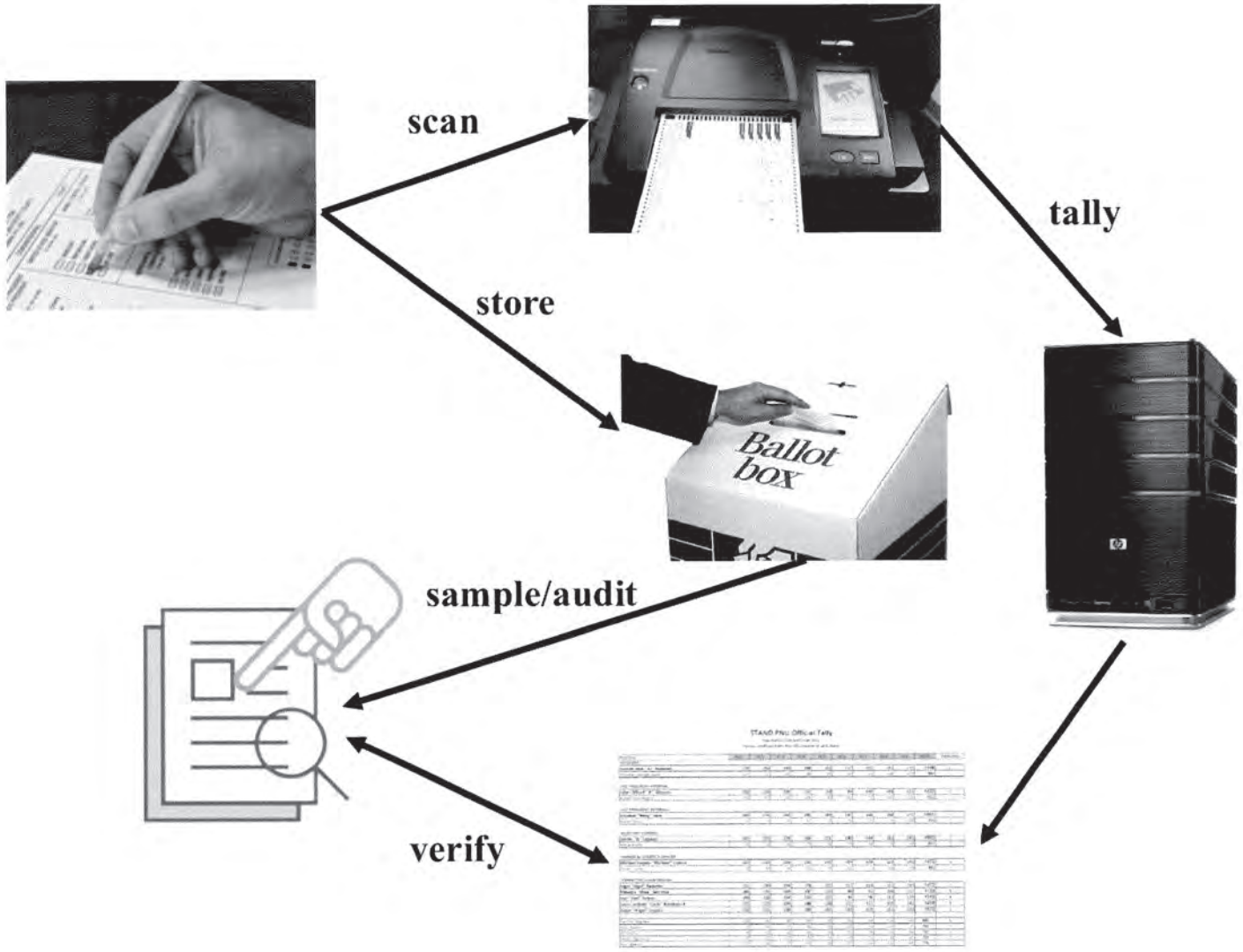
- Specification and Design
  - Strong software independent
    - An undetected change or error (including cyberattack) in software cannot cause an *undetectable* change or error in an election outcome; and
    - A detected change or error (due to software) can be corrected without rerunning the election
    - Can recover from cyberattack but requires other trail of evidence (that cannot be affected by the software)

Cybersecurity in Voting Systems

- Specification and Design
  - Paper ballots
    - (If done right) Durable evidence to determine correct election outcome
      - Must secure the custody of paper ballots
  - Statistics and auditing
    - Continue to examine random samples of ballots, until
      - There is strong statistical evidence that the election outcome is correct, or
      - There has been a complete manual tally

Cybersecurity in Voting Systems

- Specification and Design
  - Paper ballots done right - with auditing, will accomplish:
    - Verifiably cast-as-intended
    - Verifiably collected-as-cast
    - Verifiably counted-as-collected
    - Cannot by completely controlled/manipulated by any cyber component
      - Voters commit/verify votes on ballots
      - Readable/countable by human


scan
tally
store
Ballot box
sample/audit
verify

Cybersecurity in Voting Systems

- Implementation
  - Not all cyber systems are created equal
    - Choice of hardware and operating system
    - Choice of programming language
    - Secure coding practice
    - Review (open design/source)
    - Penetration testing, bug bounty
  - Latest security technologies
    - E.g., new hardware and software components specifically designed to provide security protection
    - *Don't use the same system for more than a few years!*

Cybersecurity in Voting Systems

- Operation and maintenance
  - Adopt best practices in cybersecurity, e.g.,
    - Strong authentication and data encryption
    - Blocking and detecting bad activities at network parameters as well as endpoints
    - Up-to-date security patches
    - Penetration testing
    - Training, e.g., anti-phising